EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Shun Yao Reg. No. 59242 on 10/30/2008.

The application has been amended as follows:

2. Claim 1. A method for sharing a secure communication session, comprising, establishing a secure socket layer (SSL) session between a client and a first server, wherein the first server publishes on a database a set of session state information for the SSL session, and wherein the SSL session state information includes:

3. an SSL session identifier;

4. a read key for encrypting communications from the client;

5. a write key for encrypting communications from the first server;

6. an encrypted running message digest; and

7. a message digest key which is used to encrypt the running message digest; and

8. wherein the first server continually changes the running message digest as messages are sent through the SSL session, and wherein the first server publishes updates to the running message digest to the database;

9. receiving a message from the client at a second server, wherein the message includes the SSL session identifier which identifies the SSL session between the client and the first server, and wherein the second server contains different content and performs different functions from the first server;

10. determining that an SSL session corresponding to the received session identifier is not configured on the second server;

11. querying the database with the received SSL session identifier;

12. retrieving from the database identifier the SSL session state information which corresponds to the received SSL session identifier and which is published by the first server;[[;]]

13. establishing an SSL session between the client and the second server with the same SSL session identifier based on the retrieved SSL session state information; and

14. using the running message digest to send a second message from the second server to the client through the SSL session without establishing a separate SSL session between the client and the second server.

Allowable Subject Matter

15. The following is an examiner's statement of reasons for allowance: the closest prior art of record, (Abramson et al. 6539494, Sandhu 6985953, RFC 1321 and Kunzelman et al. 6041357), does not teach or suggest in detail, "a apparatus, storage medium or method for sharing a secure communication session, comprising, establishing a secure socket layer (SSL) session between a

client and a first server, wherein the first server publishes on a database a set of session state information for the SSL session, and wherein the SSL session state information includes:

16. an SSL session identifier; a read key for encrypting communications from the client; a write key for encrypting communications from the first server; an encrypted running message digest; and a message digest key which is used to encrypt the running message digest; and

17. wherein the first server continually changes the running message digest as messages are sent through the SSL session, and wherein the first server publishes updates to the running message digest to the database;

18. receiving a message from the client at a second server, wherein the message includes the SSL session identifier which identifies the SSL session between the client and the first server, and wherein the second server contains different content and performs different functions from the first server;

19. determining that an SSL session corresponding to the received session identifier is not configured on the second server; querying the database with the received SSL session identifier;

20. retrieving from the database identifier the SSL session state information which corresponds to the received SSL session identifier and which is published by the first server;

21. establishing an SSL session between the client and the second server with the same SSL session identifier based on the retrieved SSL session state information; and

22. using the running message digest to send a second message from the second server to the client through the SSL session without establishing a separate SSL session between the client and the second server," as argued by the Applicant and found in the Specification (see Remarks

dated 09/08/2008, pages 7-10; Specification as of 11/09/2006, pages 9-14; and Drawings dated 03/30/2000, Figures 1-6 of Applicant's enabling portions of the specification and drawings).

23. The prior art of Abramson, Sandhu, RFC 1321 and Kunzelman do not teach the Applicant's claimed invention in regards to the SSL session state information includes:

24. an SSL session identifier; a read key for encrypting communications from the client; a write key for encrypting communications from the first server; an encrypted running message digest; and a message digest key which is used to encrypt the running message digest; and

25. wherein the first server continually changes the running message digest as messages are sent through the SSL session, and wherein the first server publishes updates to the running message digest to the database;

26. receiving a message from the client at a second server, wherein the message includes the SSL session identifier which identifies the SSL session between the client and the first server, and wherein the second server contains different content and performs different functions from the first server;

27. determining that an SSL session corresponding to the received session identifier is not configured on the second server; querying the database with the received SSL session identifier;

28. retrieving from the database identifier the SSL session state information which corresponds to the received SSL session identifier and which is published by the first server;

29. establishing an SSL session between the client and the second server with the same SSL session identifier based on the retrieved SSL session state information; and

30. using the running message digest to send a second message from the second server to the client through the SSL session without establishing a separate SSL session between the client and the second server.

31. Abramson teaches a three tier server system that utilized a web server, application server and a backup server that uses session IDs encoding IP addresses and switching between servers for their specific functions. Abramson does not teach the use of this type of session migration with the same session ID nor same session. Abramson teaches in column 4, line 40 et seq., that session data is reconstituted into a newly created session, with a new session ID. This is clearly not what the Applicant's invention of utilizing the same session ID and information to switch from different servers.

32. Sandhu teaches similar type of session migration as Abramson but with the use of cookies to aid in a type session ID. Sandhu teaches the use of encryption to encrypt a cookie and sharing keys to the appropriate nodes to de-crypt those cookies. This is not the same as sharing the SSL session ID since there is no SSL session created in the application.

33. Sandhu teaches the use of a message digest, i.e., MD5 or SHA, see column 3, lines 55 et seq., but does not utilize the technology the same way as the Applicant. It is clear that the Applicant utilizes this technology to continually encrypt the SSL session ID information that is shared with other servers. This is not the case in Sandhu as can be seen in their columns. Sandhu teaches using the message digest on a cookie that is only used with a specific server. The servers do not share a session ID only how the cookie was encrypted, i.e., keys, which is a common encryption tool.

34. RFC 1321 merely expands on what a message digest is and how it is used. Utilized in combination with Sandhu, which teaches the initial use of a message digest, and Abramson does not remedy the missing teachings that the claims state.

35. Kunzelman, which was used in a previous rejections and is considered pertinent prior art and has similar teachings as the claimed invention, teaches migrating from one server to another. The means of which are different from the claimed invention. Kunzelman teaches the use of a session token, table 1, which is generated when a client makes a selection which their server A determines as a migration. Server A sends the token to the client and then to server B. If there is more information needed, server B requests it from server A using the session token. This is not the same as the teachings of the claimed invention, i.e., a separate database stores all information needed for the session migration and the user has no interaction with the requesting of session information from a second server. Furthermore, the information used in the session token creates a new session between the client and server B, column 6, and does not continue the session as described by the Applicant's invention, i.e., the Applicant's claimed invention prevents the need to create a new session. Furthermore, Kunzelman does not teach the use of running message digests to aid in the encryption of the SSL session identifier as stated in the Applicant's claimed invention.

36. The cited areas of the prior art clearly do not find the Applicant's invention obvious and would be difficult to motivate one of skill in the art to combine these used references to come up with the Applicant's claimed invention.

37. The dependent claims further limit the independent claims and are considered allowable on the same basis as the independent claim as well as for the further limitations set forth.

38. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

39. Claims 1, 10, 13, 22, 25 and 33 are allowed.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DAVID E. ENGLAND whose telephone number is (571)272-3912. The examiner can normally be reached on Mon-Thur, 7:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tonia Dollinger can be reached on 571-272-4170. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

David E. England
Examiner
Art Unit 2443

/David E. England/
Examiner, Art Unit 2443